Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of claims:

Claim 1 (previously presented): A method of verifying data integrity between at least two correspondents in a cryptographic scheme, at least one of said at least two correspondents having a main processor and a secure module, said secure module being independent of said main processor's control, said method comprising the steps of:
assembling data on at least one of said at least two correspondents;
displaying said data under control of said main processor to produce a first output;
forwarding said data to said secure module and displaying said data from said secure module to produce a second output;
to permit comparison of said first output and second output; and
instructing said secure module to generate a signature on said data upon a favorable comparison of said first output and said second output;
whereby said favorable comparison indicates data integrity such that said at least one of said correspondents signs said data.

Claim 2 (original): The method of claim 1, wherein said at least one of said at least two correspondents is a personalized device.

Claim 3 (original): The method of claim 2, wherein said personalized device is a mobile phone.

Claim 4 (original): The method of claim 2, wherein said personalized device is a personal digital assistant.

Claim 5 (previously presented): The method of claim 1, wherein said favorable comparison is characterized in that said first output and said second output are logically related to one another.

Claim 6 (previously presented): The method of claim 5, wherein said logical relationship is such that said first output and said second output are identical.

Claim 7 (previously presented): The method of claim 1, wherein said step of displaying said data message includes displaying a portion of said data message.

Claim 8 (previously presented): The method of claim 7, wherein said favorable comparison is characterized in that a portion of said first output and a portion of said second output are logically related to one another.

Claim 9 (previously presented): The method of claim 8, wherein said logical relationship is such that said portion of said first output is identical to said portion of said second output.

Claim 10 (currently amended): A method of establishing a trusted communication path for data between a personalized device and a user of said device in a cryptographic scheme, said device having a main processor and a secure module independently operative of said main processor, said method comprising the steps of:
providing an interface between said device and said user, said interface having an input device and an output device for providing a means for interaction between said user and device, said input device and output device controllable by said main processor;
providing a trusted communication path between said secure module and a secure input device and a secure output device coupled thereto, said trusted path logically isolated from any other communication path;
assembling data at said input device and said secure module ~~input device~~ and forwarding said data to said ~~secure module~~ secure output device over said trusted communication path; and
displaying said data on said output device and said secure output device, to permit comparison of said data displayed on said output device and said secure output device;
whereby said user of said personalized device can determine said integrity of said data based on said comparison.

Claim 11 (original): The method of claim 10, wherein said user actuates said secure input device based only on said output of said secure output device.

Claim 12 (previously presented): A method for verifying the integrity of a data message between a correspondent and a personalized device in a communication system, each correspondent adapted to receive and transmit data messages, said method comprising the steps of:
containing a secret key in a secure module, said secure module adapted to be removably coupled to said personalized device and communicatively coupled thereto; and
controlling access to said personalized device based on a comparison of data from said secure module and data from a main processor of said personalized device, said main processor independently operable of said secure module.